UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with http://www.thehempville.com that is stored at premises controlled by Newfold Digital, Inc.

Case No. 1:22MJ 322 -1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Information associated with the website http://www.thehempville.com that is stored at premises controlled by Newfold Digital, Inc., as described in Attachment A.

located in the Middle District of Florida, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of, instrumentalities used in committing, contraband, and fruits of the crimes pertaining to violations of 18 U.S.C. Section 2252A, as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached affidavit incorporated by reference herein

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/ Zachary M. Neefe
Applicant's signature

Zachary M. Neefe, Special Agent - H.S.I.
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 8/23/2022

Judge's signature

City and state: Winston-Salem, North Carolina

JOI ELIZABETH PEAKE, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH HTTP://WWW.THEHEMPVILLE.COM THAT IS STORED AT PREMISES CONTROLLED BY NEWFOLD DIGITAL, INC.	Case No. 1:22MJ322

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Zachary M. Neefe, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Bluehost, Inc., a subsidiary of Newfold Digital, Inc., an electronic service provider headquartered at 5335 Gate Parkway, Jacksonville, Florida 32256. The particular account associated with this search warrant is the hosted website content associated with the following website address: http://www.thehempville.com (the "TARGET ACCOUNT"). The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Newfold

Digital, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI") since February of 2020 and am currently assigned to the Winston-Salem, North Carolina, Office of the Resident Agent in Charge. Prior to working with HSI, I was a detective and federal task force officer for over two years at the Alamance County Sheriff's Office in North Carolina where I specialized in child exploitation and sexual abuse investigations.

3. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training facilitated by the Internet Crimes Against Children ("ICAC") Task Force, at the National Cybercrimes Center ("C3"), and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography, child exploitation, and sex trafficking and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer

media. My training through C3 and the ICAC Task Force has included undercover chats for child exploitation cases, peer-to-peer file sharing of child pornography, online ads pertaining to enticement of children, and training specific to the BitTorrent file sharing technology. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2252A (relating to child pornography), and I am authorized by law to request a search warrant.

4. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located inside the electronic data contained in the TARGET ACCOUNT.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, § 2252A have been committed using the TARGET ACCOUNT. There is also probable cause to search the information described

in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes further described in Attachment B.

STATUTORY AUTHORITY

6. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252A(a)(2)(A), (B) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or

transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions are applicable to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

d. The term "hyperlink" refers to a term in computing where a given link provides access to another location by clicking or accessing the link. An Internet address auto-formatted by Microsoft Word (e.g. http://www.google.com) is an example of a hyperlink. The recipient of the address (in this case, the reader of this affidavit if reading on a digital device) can click on the text of the address, which "links" to the target website (Google.com).

e. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. An "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent

from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

g. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their subscribers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

h. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

i. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to,

microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

j. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic area of any person.

k. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that

has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON WEBSITE HOSTING / DIGITAL DOMAINS

8. Web hosting companies, such as http://www.bluehost.com, maintain server computers connected to the Internet. Their subscribers use those computers to operate websites on the Internet.

9. In general, web hosting companies like http://www.bluehost.com ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone number and other identifiers, e-mail addresses, and business information. Web hosting companies also may retain records of the length of service (including start date) and types of services utilized. In addition, for paying subscribers, web hosting companies typically retain information about the subscribers' means and source of payment for services (including any credit card or bank account number).

10. Web hosting companies' subscribers place files, software code, databases, and other data on the servers. To do this, subscribers connect from their own computers to the server computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a subscriber to upload files using a special website interface offered by the web

hosting company. It is frequently also possible for the subscriber to directly access the server computer through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Subscribers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses ("IP addresses") of the remote users' computers (IP addresses are used to identify computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

11. The servers use those files, software code, databases, and other data to respond to requests from Internet users for pages or other resources from the website. Commonly used terms to describe types of files sent by a server include HyperText Markup Language ("HTML") (a markup language for web content), Cascading Style Sheets ("CSS") (a language for styling web content), JavaScript (a programming language for code run on the subscriber's browser), and image files. Web hosting companies frequently allow their subscribers to store collections of data in databases. Software running on the

web server maintains those databases; two common such programs are named MySQL and PostgreSQL, although these are not the only ones.

12. Web hosting companies sometimes also provide their subscribers with e-mail accounts; contents of those accounts are also stored on the web hosting company's servers.

13. Web sites deliver their content to users through the Hypertext Transfer Protocol ("HTTP"). Every request for a page, image file, or other resource is made through an HTTP request between the subscriber and the server. The server sometimes keeps a log of these HTTP requests that shows the subscriber's IP address, the file or resource requested, the date and time of the request, and other related information, such as the type of Web browser the subscriber uses.

14. Web sites are often known to the outside world by a domain name, such as www.uscourts.gov or www.amazon.com. Domain names must be registered to particular individuals. Sometimes, web hosting companies offer subscribers the separate service of registering domain names. When that occurs, web hosting companies typically retain information related to the domain name, including the date on which the domain was registered, the domain name itself, contact and billing information for the person or entity who registered the domain, administrative and technical contacts for the

domain, and the method of payment tendered to secure and register the domain name.

15. In some cases, a subscriber or user will communicate directly with a web hosting company about issues relating to a website or account, such as technical problems, billing inquiries, or complaints from other users. Web hosting companies typically retain records about such communications, including records of contacts between the user and the company's support services, as well as records of any actions taken by the company or user as a result of the communications.

SUMMARY CONCERNING PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT, AND DISTRIBUTION OF CHILD PORNOGRAPHY

16. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction

from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines,

correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts, or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer-to-Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

h. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To

distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

i. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones, and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

j. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer (via a USB cable) or connect with a computer via Bluetooth, and transfer data files from one digital device to another. Some "smartphone" users can and do create, communicate, upload, and download child pornography, and communicate with children to coerce

them or entice them to produce child pornography or perform sexual acts, by using internet based social media or electronic service providers like Instagram, Snapchat, or Apple (and many others).

k. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

l. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, LLC, Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet.

Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

m. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

n. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over a terabyte of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

o. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost.

Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

p. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused

after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

q. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and on the evidence of known Internet-based communications further described below, there exists a fair probability that evidence regarding the receipt and possession of child pornography will be found in the website accounts that are the subject of this search warrant, namely thehempville.com, notwithstanding the passage of time.

PROBABLE CAUSE

Crimestoppers Tip Leads to Discovery of Child Pornography on Commercial Website

17. On August 15, 2022, Homeland Security Investigations (HSI) Winston-Salem Special Agent (SA) Zachary Neefe (your affiant) was contacted by Gibsonville Police Department (GPD) Detective Travis Sykes[1] in reference to a child exploitation matter. TFO Sykes explained that his department had received an Alamance Crimestoppers Tip from an anonymous person, hereinafter referred to as the Source of Information (SOI), identifying Taimour AZHAR (later confirmed to have the same legal name, O/M, DOB: 07/05/1985, NCOLN: 35682911) as sharing child sexual abuse material (CSAM[2] / child pornography) via a website.

18. In further investigating the incident, TFO Sykes requested HSI assistance for logistical support, subject matter expertise, and computer forensic capabilities. TFO Sykes and I went over the Crimestoppers Tip during the morning of August 15, 2022. The Crimestoppers Tip, identified as Tip 1282W1700, read as follows:

---

[1] Det. Sykes is a federal cross designated HSI Task Force Officer ("TFO") out of the HSI Winston-Salem Office under 19 U.S.C. § 1401, as are the additional TFOs identified further within this affidavit.

[2] Child sexual abuse material, aka "CSAM," is the industry best-practice terminology for the images and videos meeting the United States Code definition of child pornography.

"I met a guy named Taimour Azhar on Tinder. He started talking about his fetishes and he said he would show me his fetish via email with pictures. I gave him my email address and he sent me links to child porn. The links are from his business website. He says he's the CEO of thehempville.com. It looks like he's storing these images on his website in private folders. He lives in Elon, NC. He also mentioned he had two small children of his own."

19. After this, TFO Sykes and I reviewed two hyperlinks present within additional info in the Crimestoppers Tip. TFO Sykes viewed and summarized the two hyperlinks within the Crimestoppers Tip as follows, which I personally observed was accurate and consistent with my subsequent review of the CSAM imagery:

Upon review of the tip, there were two (2) links to a website, and clicking one of the links provided in the tip, I was directed to the following website: https://thehempville.com/iaceinc/bin/image5.PNG
This website contained a picture in PNG format. It was a picture of what appeared to be a female that appears to be 6 to 8 years of age. It is important to note that the picture shows the female on her back, and from about her belly button to her feet are showing. She is naked and sitting

with her legs spread open and her legs are drawn up and off of what appears to be a bed. There is a hand, which appears to be from a Caucasian male, you can only see the top of his hand, about the knuckles to the fingers. It appears to be his right hand, and his index finger is pointed, the rest are curled under his palm. His index finger is inserted into the female's vagina where you can see the tip of his finger is inside of her. The vagina appears to have lube on and around it. The female's right hand is also pictured, it is on her right hip, her index finger appears to have lube on it as well, and the fingers are spread apart with her thumb near her belly button and her index finger beside of her vagina and the other three fingers are on her leg. There are no further details in the picture that would lead to an identification of the female or male subject in the photo.

The other link in the tip was the following website: https://thehempville.com/iaceinc/bin/image10.PNG

This website contained a picture in PNG format. It was a picture of what appeared to be a female that appears to be 8 to 10 years old. She is standing in what appears to be a bedroom. The bedroom has white walls, a picture in the background of what may be a tree in a frame, is behind her to her right. She is facing the camera, and there appears to be a couch

to her left and behind her. There is also what appears to be a ceiling fan in the room, the blade appears behind her head, and there is a crystal hanging from the fan. The room appears to be white, and dark, not well lit. The female is standing, her hands are behind her back, and her right leg is up on something with both legs spread. She is completely naked and has what appears to be panties in her mouth. The panties are multicolored and appear dark blue and light blue. The female is blonde with her hair down but pulled back. She is completely nude, and you can see her vagina as well as both breasts.

Search Warrant at AZHAR's Residence in Gibsonville City Limits

20. After this, TFO Sykes and I worked to develop an operational plan for the execution of a residential search warrant at AZHAR's residence later in the day. AZHAR'S residence was identified via database records checks, including the North Carolina Division of Motor Vehicles, North Carolina Secretary of State (business officer records), and physical surveillance. Additionally, utility records indicated that AZHAR's status at the residence appeared current up until the present time. Meanwhile, I submitted a preservation request to GoDaddy.com, which appeared to be the domain host

for thehempville.com[3] website indicated in the Crimestoppers Tip. Additional preservation requests were submitted for the associated Gmail accounts and other social media identifiers discovered during subsequent open-source intelligence gathering.[4] These accounts were preserved in the event that they became relevant to this investigation.

21. On the afternoon of August 15, 2022, HSI, GPD, and Alamance County Sheriff's Office (ACSO) executed a state search warrant for AZHAR's residence, signed by North Carolina Superior Court Judge Andy Hanford a short time before. Personnel present known to me included the following: myself (SA Neefe), TFO Sykes, TFO Joshua Hartong, TFO Michael Hargrove, ACSO Det. Zoe Wood, ACSO Det. Hiram Coble, ACSO Det. Gary Williams, and GPD Lt. Alan Warf.

---

[3] GoDaddy appeared to be the domain host for thehempville.com based on WHOIS Internet queries. WHOIS databases, short for "Who is responsible for this domain?", are available from different registrars, and provide a starting point for understanding who is responsible for registering and hosting a website. Some companies provide all-inclusive hosting services, to include domain registration, hosting, email services, and other back-end administrative tasks. Other registering/hosting companies will provide more limited services, with the hosting and website registration administered by different companies.

[4] thehempville.com appears to be a legitimate website, connected with Hempville of North Carolina LLC, a private business registered with the State of North Carolina to AZHAR. Based on the website's "ABOUT US" tab and in-person conversations with AZHAR, Hempville of NC is a research and development company that markets agricultural hemp products to other businesses. Hempville of NC engages in contractual consulting services for public/private entities (other private businesses as well as public universities). Since AZHAR is an engineer by profession, the consulting he provides mainly focuses on industrial applications and bringing new hemp products to market (e.g. textile replacement of hemp over cotton, bioplastics, hemp edible products).

22. When TFO Sykes and I knocked on the door of AZHAR's residence (15 Silver Maple Drive, Elon, NC 27244[5]), AZHAR came to the door accompanied by a large dog. The dog was not aggressive and was restrained by AZHAR with officers then accompanying AZHAR into the residence. AZHAR then stated that he had two (2) children present at home with him. The children were safely escorted to a rendezvous location within the residence while a safety sweep was conducted by other law enforcement officers on-scene.

23. Once it was determined that there were no other individuals present at the house, AZHAR was interviewed by TFO Sykes and I. AZHAR's children were supervised by other law enforcement officers with AZHAR being allowed to occasionally check in on his kids throughout the non-custodial interview. Although the interview was non-custodial in nature, I nonetheless recited and received verbal waiver of Miranda Rights from AZHAR. The interaction with AZHAR was memorialized in the form of handwritten notes (mine) and a body camera (TFO Sykes). Both the notes and recording will be retained with the case file for this investigation.

24. AZHAR was polite and cooperative throughout law enforcement's interaction with him on-scene. He appeared sober and of sound mind; however, AZHAR had a noticeable injury to his foot and was walking with a cane

[5] Although this address is serviced by the Elon, NC Post Office, it is territorially within the primary jurisdiction of the Town of Gibsonville, NC.

throughout law enforcement's interaction with him. AZHAR stated that he had broken his foot and was still recovering from the injury.

25. AZHAR was allowed to call, and subsequently interacted with Attorney Bryan Ray while law enforcement was on-scene. This was prior to any questions taking place. I then asked AZHAR if he wished to record Attorney Ray's information. AZHAR stated he did not need to as he had Attorney Ray's information memorized. Since all electronic devices were listed as "Items to be Seized/Searched" in TFO Sykes' search warrant, AZHAR's phone was then placed in airplane mode and handed off to computer forensic personnel on-scene for initial forensic previewing.

26. AZHAR read through the search warrant and adamantly denied being involved in child exploitation. Due to an ongoing divorce and child custody dispute, AZHAR stated that he thought someone may have "hacked" his website or otherwise set him up to look bad. AZHAR maintained that he was a legitimate business owner and possessed neither the technical skills nor desire to upload CSAM to his website. He stated that the anonymous method used to implicate him was a clear sign that someone from his ex-wife's family or an associate was the likely accuser.

27. AZHAR made no incriminating statements regarding possible sexual interest in children. AZHAR identified as a straight, heterosexual male interested only in adult females. AZHAR provided no particular "type" or

sexual fetishes of interest, stating at one point that a "woman's a woman" and that he had had no difficulty fulfilling his sexual interests in the past months. AZHAR said he was currently in a sexual dating relationship with a female and that because of this relationship, he had no need to seek out random dates via online dating. AZHAR admitted to having installed and previously paying for a premium Tinder account (the same application identified in the Crimestoppers Tip) but said he had never actually met anyone in-person from Tinder and had used the identifier "Tee" on the app – not his real name. AZHAR denied ever having viewed child pornography and stated he rarely viewed adult, legal pornography, going months at a time without viewing pornography.

28. AZHAR identified the following accounts as being his own during the interview: Taimour.Azhar@gmail.com, sales@thehempville.com (old account, the company no longer uses @thehempville.com email addresses due to spam), thehempville@gmail.com[6], Taimour.Azhar@Rockwellautomation.com (email for a full-time job he has as an engineer).

[6] Of special note, this email address, "thehempville@gmail.com", was/is listed as the "Contact Us" email address on thehempville.com for the duration of this investigation. The email address is present on the right side of the website's bottom banner, which appears to be formatted to be displayed at the bottom of every page.

29. Regarding the website itself, AZHAR stated that the website thehempville.com is for his legitimate hemp consulting business. AZHAR identified Hempville as having contractual obligations with NC State University and other institutions for which he has provided consulting services. AZHAR stated that there had been numerous issues with spam in the website's email and the website crashing; therefore, over the course of the company's existence, there had been no fewer than four (4) web developers or administrators, including the ex-brother-in-law whom he thought may have framed him for CSAM sharing/possession. The current website administrator was identified by AZHAR as being a freelancer in Pakistan (AZHAR's birthplace). The freelancer "Usman" was receiving $1,000 monthly for maintenance on the website as well as social media posts/influencing. AZHAR also stated he paid a $250 yearly fee to BlueHost[7] to host the website.

30. Ultimately, there was no CSAM imagery recovered on-scene and the computer forensics are still pending as of the time of this affidavit. A check of the CSAM URLs above with a forensic computer have revealed a "page not found" error on thehempville.com website now, suggesting that someone is attempting to alter the website in order to hide/destroy evidence.

---

[7] The hosting relationship between GoDaddy and BlueHost Inc. was not fully understood by investigators at the time of this initial interview. See further in the affidavit for additional explanation of the data's physical location and the contractual relationships between GoDaddy and BlueHost Inc.

Additional Investigative Steps & Follow Up

31. In follow up with Alamance County Crimestoppers, TFO Sykes reported that the Crimestoppers software/website is setup to anonymize any incoming reports. The device information and IP logs are "scrambled" by the Crimestoppers system in an effort to prevent law enforcement from identifying reporting parties. Therefore, it appears that it is not possible to positively identify the reporting party (and possible suspect if this is a false report / conspiracy) from Crimestoppers records.

32. In a phone conversation follow up with GoDaddy representative Keena Willis and subsequent email follow up with GoDaddy representative Danielle Baker (both interactions occurring on August 16, 2022), I learned that while GoDaddy likely marketed and maintained basic subscriber information on thehempville.com website, the data itself for the website was housed on BlueHost, Inc. servers. The representatives explained that oftentimes the entity storing the website's contents (leased server space) is different than the company marketing and accepting payment for webhosting, similar to a sublet on a lease. Although GoDaddy received a preservation request, both representatives stated that a preservation request (and subsequent legal process) would need to be served on BlueHost, Inc. in order to avoid a loss of data and potential evidence.

33. With this in mind, I submitted a preservation request via email to BlueHost, Inc. on August 16, 2022. BlueHost, Inc. Data Request representative Jenessa Smith responded by email and stated that BlueHost, Inc. is a subsidiary company of Newfold Digital, Inc. and that any requests or legal processes would need to be issued to that company. I subsequently submitted a preservation request to Newfold Digital, Inc. and began work on a search warrant in reference to the contents of thehempville.com website.

34. This search warrant seeks information as described in Attachment B since July 15, 2022 until present. The date "July 15, 2022" was chosen as a month before the Crimestoppers Tip in order to better capture change logs, IP logs, website administrator logins, postings, support tickets, and/or other possible electronic records on thehempville.com website to establish attribution and ownership of the specific pages containing CSAM imagery.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Newfold Digital, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of

Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

36. Because the warrant will be served on Newfold Digital, Inc. who will then compile the requested records at a time convenient to Newfold Digital, Inc., reasonable cause exists to support execution of the requested warrant at any time day or night.

CONCLUSION

37. Based upon the specific facts and circumstances outlined in this investigation, as well as the conduct of individuals who have a sexual interest in children, there is probable cause to believe that the information associated with the TARGET ACCOUNT, stored at premises owned, maintained, controlled, or operated by Newfold Digital, Inc., contains evidence of violations of 18 U.S.C. § 2252A; I therefore respectfully request that a warrant be issued for the search of the account described in Attachment A, for the search and seizure of the items more fully described in Attachment B and request that the Court issue the proposed search warrant.

38. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction," as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A). Specifically, this Court is "a district court of the United States. . .that – has jurisdiction over the offense being investigated."

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

/S/ Zachary M. Neefe
Zachary M. Neefe
Special Agent
Homeland Security Investigations

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.

8/23/2022

The Honorable Joi Elizabeth Peake
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

This warrant applies to information associated with http://www.thehempville.com that is stored at premises owned, maintained, controlled, or operated by Bluehost, Inc., a subsidiary of Newfold Digital, Inc., a company headquartered at 5335 Gate Parkway, Jacksonville, Florida 32256.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Bluehost, Inc., a subsidiary of Newfold Digital, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Bluehost, Inc., a subsidiary of Newfold Digital, Inc., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Bluehost, Inc., a subsidiary of Newfold Digital, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Bluehost, Inc., a subsidiary of Newfold Digital, Inc., is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. all records or other information pertaining to that account or identifier, including all files, databases, and database records stored by Bluehost, Inc., a subsidiary of Newfold Digital, Inc., in relation to that account or identifier;

b. all information in the possession of Bluehost, Inc., a subsidiary of Newfold Digital, Inc., that might identify the subscribers related to those accounts or identifiers, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the

length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. all records pertaining to the types of service utilized by the user,

d. all records pertaining to communications between Bluehost, Inc., a subsidiary of Newfold Digital, Inc., and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, contraband, and instrumentalities of violations of 18 U.S.C. § 2252A (pertaining to child pornography), involving an unknown suspect since July 15, 2022, relating to the development, publishing, advertisement, access, use, administration or maintenance of child pornography or child sexual abuse material (CSAM) on any website enumerated in Attachment A, and the identity of any individuals responsible for child pornography or CSAM on such website, as follows:

1. files, databases, and database records stored by Bluehost, Inc., a subsidiary of Newfold Digital, Inc., on behalf of the subscriber or user operating the website (the hempville.com), including:

a. programming code used to serve or process requests made via web browsers, to identify individuals who are responsible for posting child pornography or CSAM on the website;

b. HTML, CSS, JavaScript, image files, or other files, to locate potential child pornography or CSAM, and/or to identify individuals who are responsible for posting child pornography or CSAM on the website;

c. HTTP request and error logs, to identify individuals who are responsible for posting child pornography or CSAM on the website;

b. SSH, FTP, or Telnet logs showing connections related to the website, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports, to identify individuals who are responsible for posting child pornography or CSAM on the website;

e. MySQL, PostgreSQL, or other databases related to the website, to locate potential child pornography or CSAM, and/or to identify individuals who are responsible for posting child pornography or CSAM on the website;

2. Subscriber information related to the accounts established to host the site enumerated in Attachment A, to include:

a. Names, physical addresses, telephone numbers and other identifiers, email addresses, and business information;

b. Length of service (including start date), types of service utilized, means and source of payment for services (including any credit card or back account number), and billing and payment information;

c. If a domain name was registered on behalf of the subscriber, the date that the domain was registered, the domain name, the registrant information, administrative contact information, the technical contact information and billing contact used to register the domain and the method of payment tendered to secure and register the Internet domain name.

III. Method of delivery

Bluehost, Inc., a subsidiary of Newfold Digital, Inc., shall disclose responsive items seized pursuant to this search warrant, if any, by sending (notwithstanding Title 18, United States Code, Section 2252A, or similar statute or code) via an encrypted online means (in accordance with industry best practices) to the Special Agent, or alternatively, via on a digital media device through the United States Postal Service or commercial interstate carrier to the following mailing/physical address:

Special Agent Zachary Neefe
Homeland Security Investigations RAC Winston-Salem
426 Gallimore Dairy Rd. Ste. 100
Greensboro, NC 27409